Ransomware Attacks Continue in Ukraine with Mysterious WannaCry Clone

bleepingcomputer.com/news/security/ransomware-attacks-continue-in-ukraine-with-mysterious-wannacry-clone/

Catalin Cimpanu

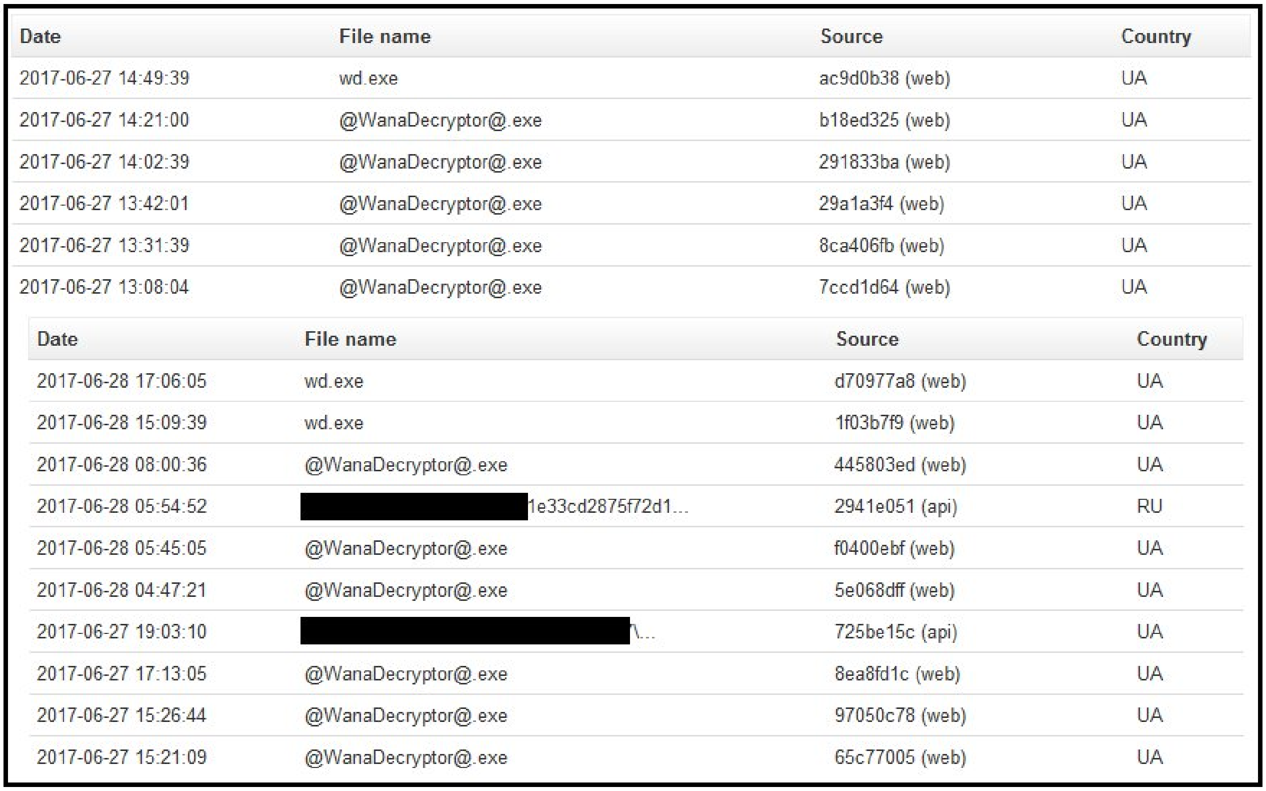
By
Catalin Cimpanu

- June 29, 2017
- 07:05 PM
- 2

A fourth ransomware campaign focused on Ukraine has surfaced today, following the same patterns seen in past ransomware campaigns that have been aimed at the country, such as XData, PScrypt, and the infamous NotPetya.

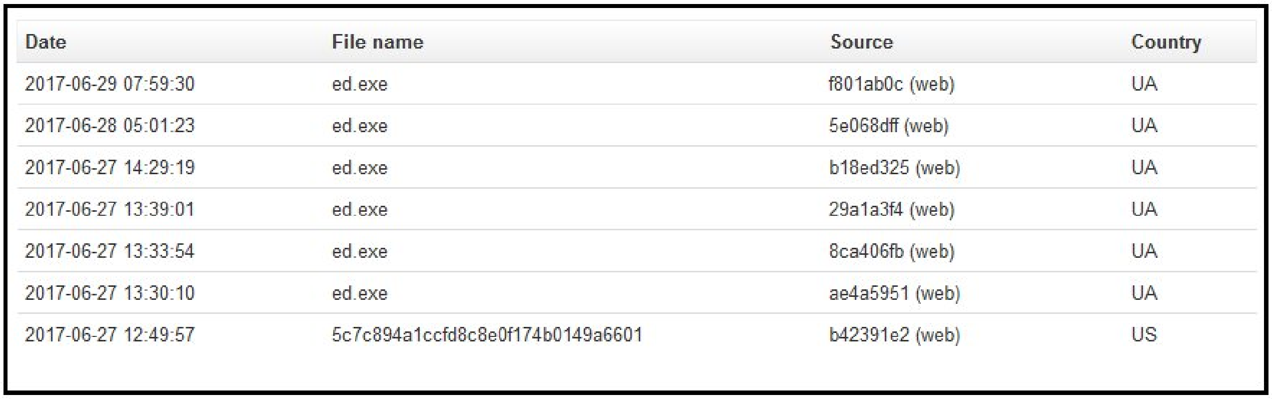
The ransomware was discovered today by a security researcher who goes online only by the name of MalwareHunter.

The researcher says the ransomware got his attention because mostly Ukrainian victims were submitting samples for analysis on VirusTotal.



Date	File name	Source	Country
2017-06-27 14:49:39	wd.exe	ac9d0b38 (web)	UA
2017-06-27 14:21:00	@WanaDecryptor@.exe	b18ed325 (web)	UA
2017-06-27 14:02:39	@WanaDecryptor@.exe	291833ba (web)	UA
2017-06-27 13:42:01	@WanaDecryptor@.exe	29a1a3f4 (web)	UA
2017-06-27 13:31:39	@WanaDecryptor@.exe	8ca406fb (web)	UA
2017-06-27 13:08:04	@WanaDecryptor@.exe	7ccd1d64 (web)	UA

Date	File name	Source	Country
2017-06-28 17:06:05	wd.exe	d70977a8 (web)	UA
2017-06-28 15:09:39	wd.exe	1f03b7f9 (web)	UA
2017-06-28 08:00:36	@WanaDecryptor@.exe	445803ed (web)	UA
2017-06-28 05:54:52	[redacted]	2941e051 (api)	RU
2017-06-28 05:45:05	@WanaDecryptor@.exe	f0400ebf (web)	UA
2017-06-28 04:47:21	@WanaDecryptor@.exe	5e068dff (web)	UA
2017-06-27 19:03:10	[redacted]	725be15c (api)	UA
2017-06-27 17:13:05	@WanaDecryptor@.exe	8ea8fd1c (web)	UA
2017-06-27 15:26:44	@WanaDecryptor@.exe	97050c78 (web)	UA
2017-06-27 15:21:09	@WanaDecryptor@.exe	65c77005 (web)	UA



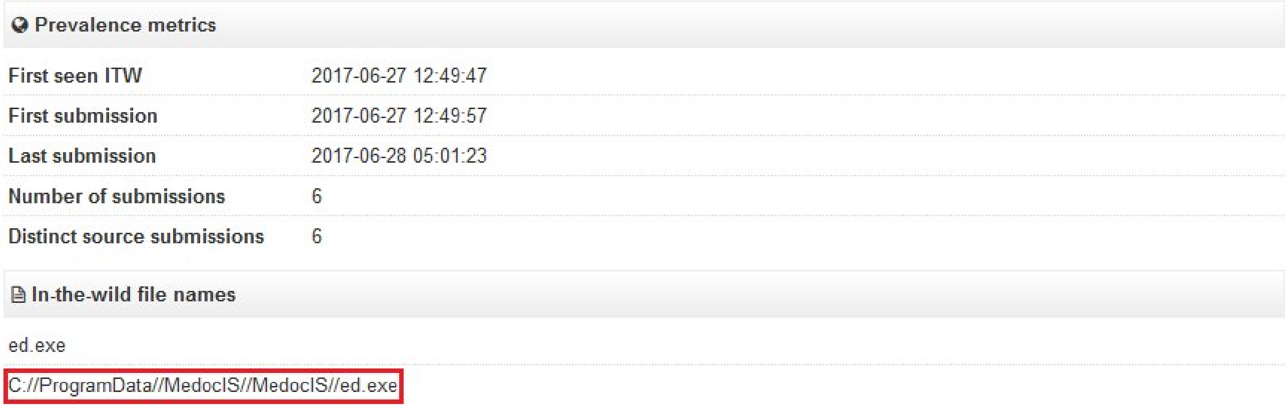
Date	File name	Source	Country
2017-06-29 07:59:30	ed.exe	f801ab0c (web)	UA
2017-06-28 05:01:23	ed.exe	5e068dff (web)	UA
2017-06-27 14:29:19	ed.exe	b18ed325 (web)	UA
2017-06-27 13:39:01	ed.exe	29a1a3f4 (web)	UA
2017-06-27 13:33:54	ed.exe	8ca406fb (web)	UA
2017-06-27 13:30:10	ed.exe	ae4a5951 (web)	UA
2017-06-27 12:49:57	5c7c894a1ccfd8c8e0f174b0149a6601	b42391e2 (web)	US

In the past month and a half, Ukraine has been bombarded with ransomware campaigns. The first was XData (mid-May), the second was PSCrypt (last week), and then NotPetya (started on Tuesday).

According to the researcher, this fourth ransomware campaign started on Monday, one day before NotPetya, and piqued his interest because of several reasons.

M.E.Doc servers appear to have distributed another ransomware

The one clue that stood out was the location of the ransomware's component, which was: "*C://ProgramData//MedocIS//MedocIS//ed.exe*"



Prevalence metrics	
First seen ITW	2017-06-27 12:49:47
First submission	2017-06-27 12:49:57
Last submission	2017-06-28 05:01:23
Number of submissions	6
Distinct source submissions	6

In-the-wild file names

ed.exe

C://ProgramData//MedocIS//MedocIS//ed.exe

This file path is specific to M.E.Doc IS-pro, a software application used for accounting in Ukraine. Both XData and the NotPetya ransomware outbreaks used the update servers of M.E.Doc to deliver their ransomware payloads. Microsoft, Kaspresky, Cisco, and other cyber-security companies have specifically pinpointed M.E.Doc software update servers as the source of the NotPetya outbreak.

> We are confident that trojanized MeDoc updates were used as an infection vector against several of our users. https://t.co/5lbvNhn6KX
>
> — Costin Raiu (@craiu) June 29, 2017

It is unclear if this recently discovered ransomware reached users via a trojanized update from the same server or a trojanized M.E.Doc app installed from scratch.

Since the start of the NotPetya ransomware outbreak that affected countries all over the world, M.E.Doc has consistently denied that it ever hosted trojanized versions of its apps.

On Facebook, M.E.Doc says it enlisted the help of Cisco experts to clear its name and investigate what really happened on its servers. In an email to Bleeping Computer, the company also said it invited officers from the Department of Cyber Police to also investigate what happened.

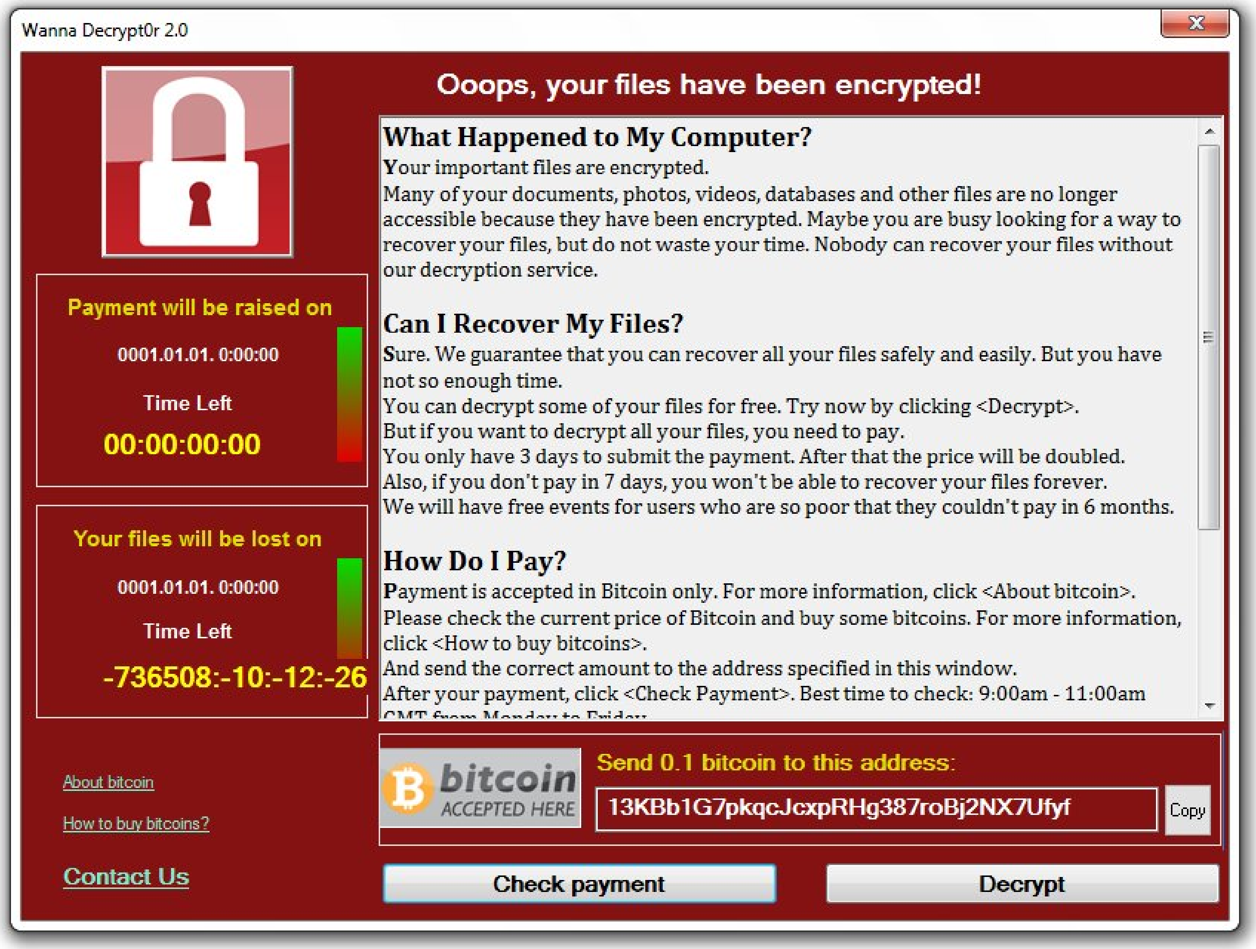
While Cisco and Ukrainian authorities are looking into identifying the real culprit behind the M.E.Doc server hijacking, it's now becoming clear that there might be another ransomware that used the same server to infect victims, albeit with less successful results than NotPetya.

"Designed" to look like WannaCry, but nothing more

This "fourth" ransomware is designed to look like WannaCry, the ransomware that affected tens of thousands of computers in mid-May.

MalwareHunter says this ransomware was "designed" to look like WannaCry, but it's not an actual clone. For starters, the ransomware is coded in .NET, while the original WannaCry was coded in C.

The WannaCry lookalike doesn't use any NSA exploits to spread laterally, and its internal structure is also different. The only thing it shares with the original WannaCry it's its GUI that shows the countdown timer and the ransom demand.



Wanna Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
0001.01.01. 0:00:00
Time Left
00:00:00:00

Your files will be lost on
0001.01.01. 0:00:00
Time Left
-736508:-10:-12:-26

Send 0.1 bitcoin to this address:
13KBb1G7pkqcJcxpRHg387roBj2NX7Ufyf

In most cases, .NET-based ransomware is usually a sign that the author has no coding experience. This is not the case with this WannaCry lookalike.

"The WannaCry lookalike is probably one of the best .NET ransomware strains we've seen," MalwareHunter says, "surely no skids made this."

The ransomware infects systems via an initial dropper that unpacks and saves two files locally, the GUI for the WannaCry-like window, and the encrypter component.

The ransomware uses a Tor-based command and control server, won't start without special command-line arguments, and will kill processes before encrypting files used in live apps. This last feature, MalwareHunter says is unique for all ransomware families he analyzed.

Someone is slinging ransomware at Ukraine

What's more peculiar is that this fourth ransomware also fits a pattern observed with the previous strains. This ransomware tries to pass as another family — WannaCry.

The same thing was noticed with XData — based on stolen AES-NI codebase; PSCrypt — based on GlobeImposter; and NotPetya — disguised as Petya.

Ransomware operators trying to pass as famous threats ain't anything new, but AES-NI and GlobeImposter are very small enterprises. There's hardly a reason for anyone to imitate these two unless wanting to go under the radar as a very very ordinary operation.

Slowly, it's becoming somewhat clear that someone is slinging ransomware specifically at Ukraine and is trying to pass as a mundane cyber crime operation, hiding other motives.

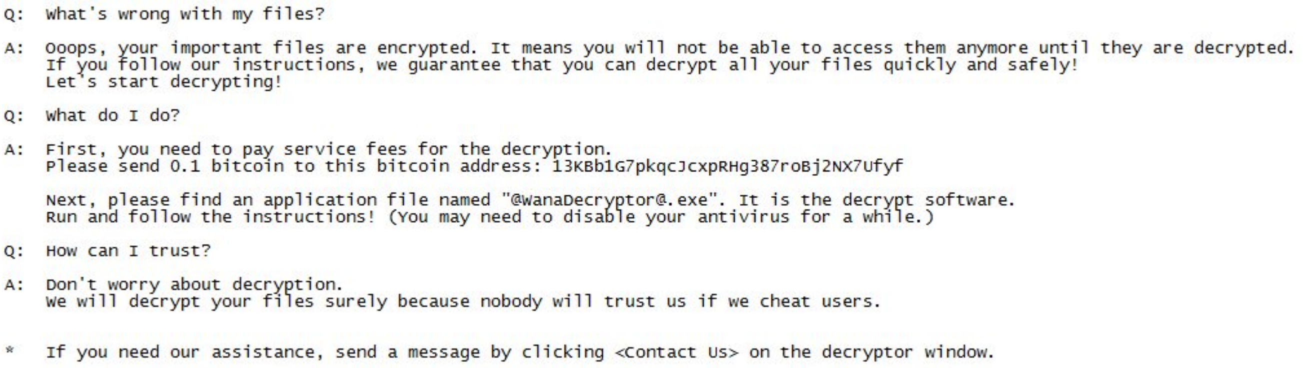
Putting all clues together, we see four ransomware campaigns that have targeted Ukraine, have tried to pass as other ransomware threats, have quality code, and three of which appear to have used the same server to spread.

There is no clear-cut evidence that the same person or group is behind all campaigns, but there are too many coincidences to ignore.

SHA256 hashes:

Dropper: 51e84accb6d311172acb45b3e7f857a18902265ce1600cfb504c5623c4b612ff
GUI: 7b6a2cbb8909616fe035740395d07ea7d5c2c0b9ff2111ae813f11141ad77ead
Encrypter: db8e7098c2bacad6ce696f3791d8a5b75d7b3cdb0a88da6e82acb28ee699175e

Ransom note:



```
Q:  What's wrong with my files?

A:  Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.
    If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely!
    Let's start decrypting!

Q:  What do I do?

A:  First, you need to pay service fees for the decryption.
    Please send 0.1 bitcoin to this bitcoin address: 13KBb1G7pkqcJcxpRHg387roBj2NX7Ufyf

    Next, please find an application file named "@WanaDecryptor@.exe". It is the decrypt software.
    Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q:  How can I trust?

A:  Don't worry about decryption.
    We will decrypt your files surely because nobody will trust us if we cheat users.


*   If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.
```

Ransom note text:

```
Q: What's wrong with my files?

A: Oooops, your important files are encrypted. It means you will not be able to
access them anymore until they are decrypted. If you follow our instructions, we
guarantee that you can decrypt all your files quickly and safely! Let's start
decrypting!

Q: What do I do?

A: First, you need to pay service fees for the decryption. Please send 0.1 bitcoin
to this bitcoin address: 13KBb1G7pkqcJcxpRHg387roBj2NX7Ufyf
Next, please find an application file named "@WanaDecryptor@.exe". It is the decrypt
software. Run and follow the instructions! (You may need to disable your antivirus
for a while.)

Q: How can I trust?

A: Don't worry about decryption. We will decrypt your files surely because nobody
will trust us if we cheat users.

* If you need our assistance, send a message by clicking < Contact Us > on the
decryptor window.
```

Update [July 4, 2017]: Kasperksy Lab has also confirmed this Bleeping Computer report.

Related Articles:

Hackers use Conti's leaked ransomware to attack Russian companies

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

- NotPetya
- Petya
- Ransomware
- Ukraine
- WannaCry
- Xdata

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Comments

-

  Demonslay335 - 4 years ago

    -
    -

  We analyzed this one to be secure as well, worth pointing out. No way to decrypt it for free without their private RSA key unfortunately.

-

  Amigo-A - 4 years ago

    -
    -

  This can be called an attack with a big stretch. Ukrainians infect computers of Ukrainians.
  This is a competitive struggle or outright sabotage. MEDoc to someone did not pay salaries, greedy, for this all customers will receive virus. This will lead to the collapse of MEDoc. Already the company is on the verge of ruin.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: